

コンバージしたアクセス (5760/3650/3850) の 設定 外部Web 認証

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[CLI 設定](#)

[GUI 設定](#)

[確認](#)

概要

この資料にコンバージしたアクセスコントローラで外部Web auth を設定する方法を定義されています。 ゲスト門脈ページおよび資格情報 認証はこの例の Identity Services Engine (ISE) に両方です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

1. Cisco はアクセスコントローラ コンバージしました。
2. Web 認証
3. Cisco ISE

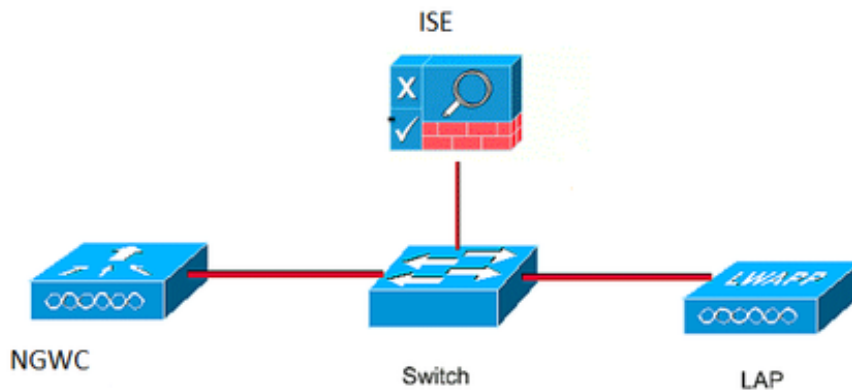
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

1. Cisco 5760 コントローラ (下記のダイアグラムの NGWC)、03.06.05E
2. ISE 2.2

設定

ネットワーク図



CLI 設定

コントローラの RADIUSコンフィギュレーション

ステップ 1: 外部の RADIUSサーバを定義して下さい

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

ステップ 2: AAA RADIUS グループを定義し、使用されるべき RADIUSサーバを規定して下さい

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

ステップ 3.半径グループを指すメソッドリストを定義し、WLAN の下でマッピングして下さい。

```
aaa authentication login webauth group ISE-Group
```

パラメータ マップ設定

ステップ 4.仮想 IP アドレスでグローバルなパラメータ マップを設定して下さい外部および内部 webauth に必要となる。Logout ボタンはバーチャルIP を使用します。その常にルーティングが不可能なバーチャルIP を設定する好ましい習慣。

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

ステップ 5: 指定されたパラメータ マップを設定して下さい。それは webauth 方式の型のように機能します。これは WLAN 構成の下で呼出されます。

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

前に認証 ACL。これはまた WLAN の下で呼出されます。

ステップ 6: 認証が終わる前に割り当てが ISE、DHCP および DNS にアクセスする Preauth_ACL を設定して下さい

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

WLAN 構成

ステップ 7: WLAN を設定して下さい

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

ステップ 8: HTTPサーバをつけて下さい。

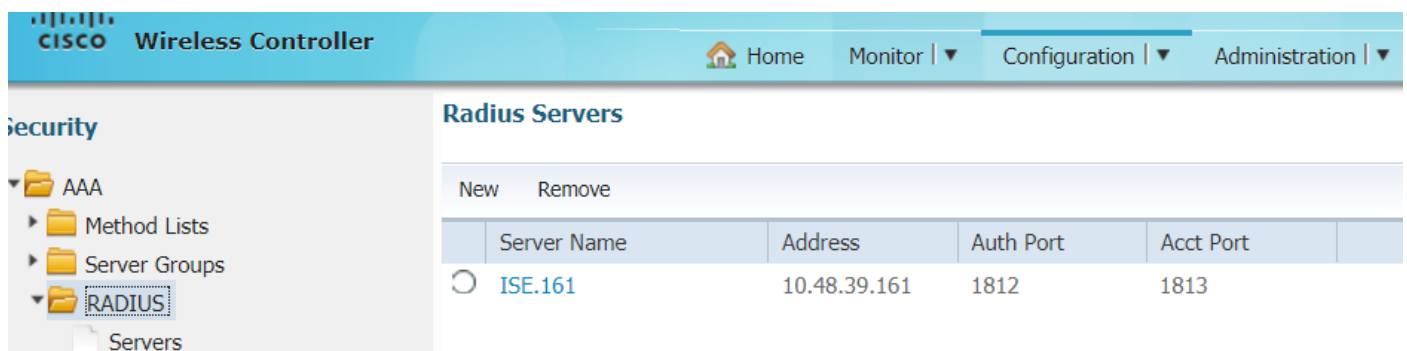
```
ip http server
```

```
ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

GUI 設定

上でここに次同じステップがあります。スクリーンショットはクロスリファレンスにちょうど提供されます。

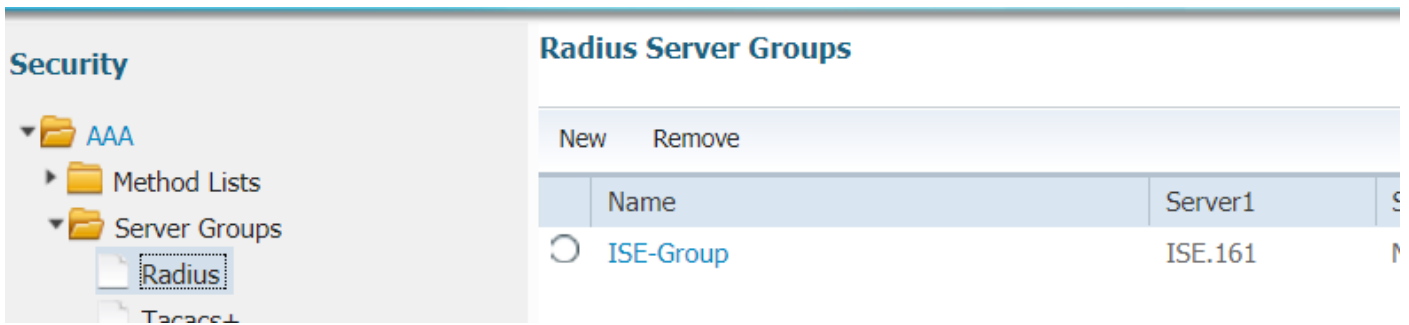
ステップ 1: 外部の RADIUSサーバを定義して下さい



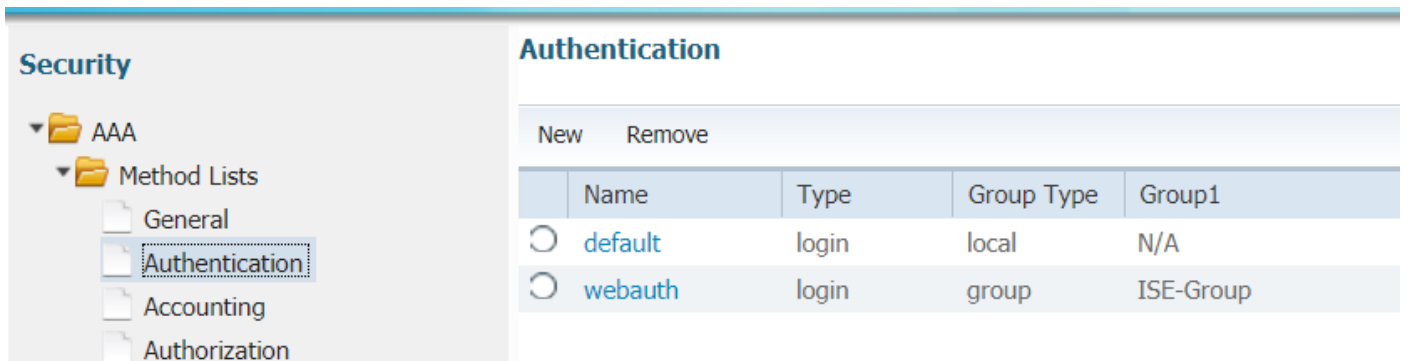
The screenshot shows the Cisco Wireless Controller GUI. The top navigation bar includes 'Home', 'Monitor', 'Configuration', and 'Administration'. The left sidebar shows a tree view with 'Security' expanded, and 'RADIUS' selected under 'Server Groups'. The main content area is titled 'Radius Servers' and contains a table with the following data:

	Server Name	Address	Auth Port	Acct Port
<input type="radio"/>	ISE.161	10.48.39.161	1812	1813

ステップ 2: AAA RADIUS グループを定義し、使用されるべき RADIUSサーバを規定して下さい



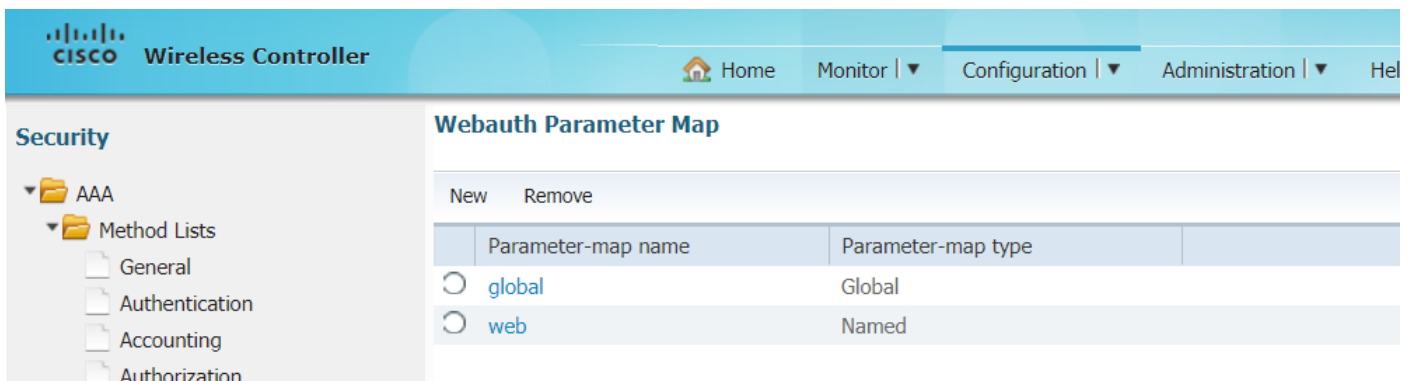
ステップ 3.半径グループを指すメソッドリストを定義し、WLAN の下でマッピングして下さい。



パラメータ マップ設定

ステップ 4.仮想 IP アドレスでグローバルなパラメータマップを設定して下さい外部および内部 webauth に必要となる。Logout ボタンはバーチャルIP を使用します。その常にルーティングが不可能なバーチャルIP を設定する好ましい習慣。

ステップ 5: 指定されたパラメータマップを設定して下さい。それは webauth 方式の型のように機能します。これは WLAN 構成の下で呼出されます。



前に認証 ACL。これはまた WLAN の下で呼出されます。

ステップ 6: 認証が終わる前に割り当てが ISE、DHCP および DNS にアクセスする Preauth_ACL を設定して下さい

CISCO Wireless Controller

Home Monitor Configuration Administration Help

Security

- AAA
 - Method Lists
 - General
 - Authentication
 - Accounting
 - Authorization
 - Server Groups
 - Radius
 - Tacacs+
 - Ldap
 - RADIUS
 - TACACS+ Servers
 - LDAP Servers
 - Users
 - Attribute List
 - MAC Filtering
 - Disabled Client
 - AP Policy
 - Local EAP
 - Wireless Protection Policies
 - CIDS
 - FQDN
 - ACL
 - Access Control Lists

Access Control Lists

ACLs > ACL detail

Details:

Name: Preauth_ACL

Type: IPv4 Extended

Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
10	permit	ip	any	10.48.39.161	-	-	-
20	permit	ip	10.48.39.161	any	-	-	-
30	permit	udp	any	any	eq 67	-	-
40	permit	udp	any	any	-	eq 68	-
50	permit	udp	any	any	eq 68	-	-
60	permit	udp	any	any	eq 53	-	-
70	permit	udp	any	any	-	eq 53	-

ext-webauth	7	ext-webauth	232	Enabled	Web-Auth
-------------	---	-------------	-----	---------	----------

WLAN 構成

ステップ 7: WLAN を設定して下さい

CISCO Wireless Controller

Home Monitor Configuration Administration

Wireless

- WLAN
 - WLANs
 - Advanced
 - Access Points
 - 802.11a/n/ac
 - 802.11b/g/n
 - Media Stream
 - QOS

WLAN

WLAN > Edit

General Security QOS AVC Policy Mapping Advanced

Layer2 Layer3 AAA Server

Web Policy

Conditional Web Redirect

Webauth Authentication List webauth

Webauth Parameter Map web

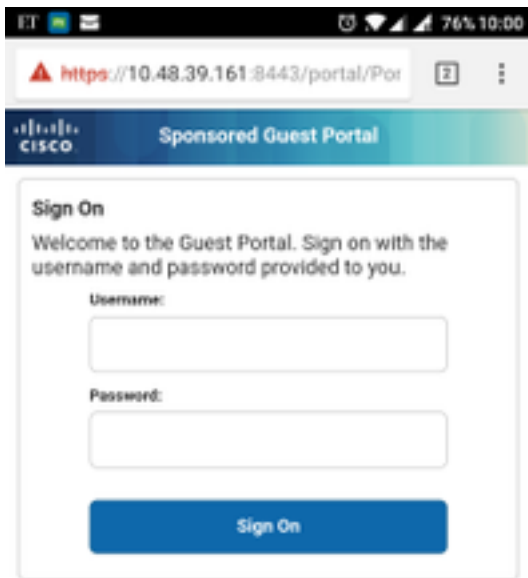
Webauth On-mac-filter Failure

Preauthentication IPv4 ACL Preauth_ACL

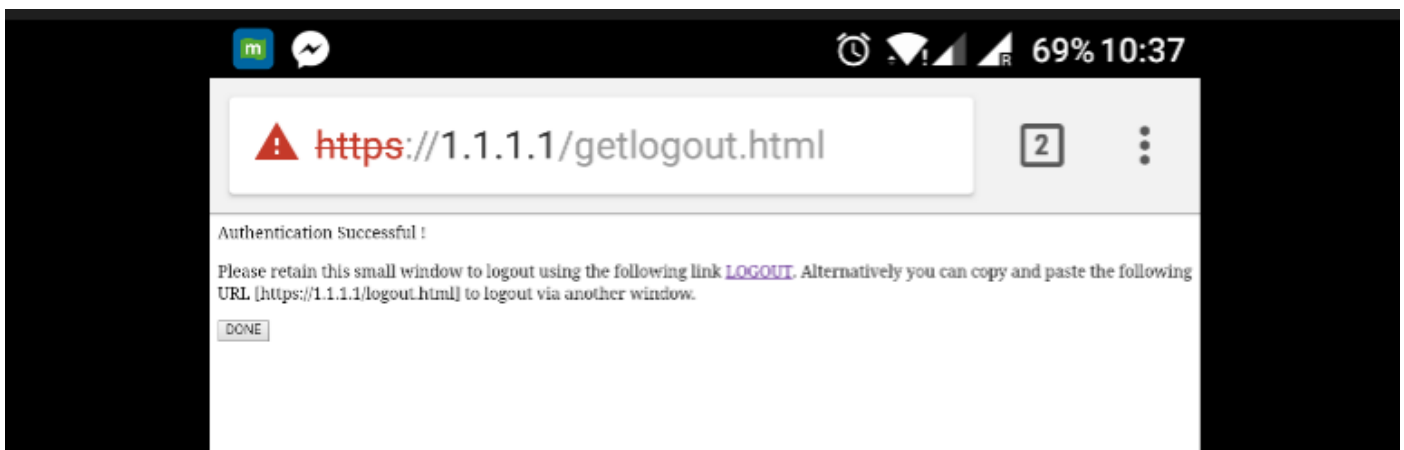
Preauthentication IPv6 ACL none

確認

ブラウザを開いたらクライアントを接続し、クライアントはログオン ポータル ページにリダイレクトされることを確かめて下さい。下記のスクリーンショットは ISE ゲスト ポータル ページを説明します。



適切な資格情報が入れば、成功ページは示されます:



ISE サーバは 2 に認証を報告します: WLC が RADIUS 認証 (このによって同じ ユーザ名/パスワードを認証だけ提供すれば guest ページの 1 つは自体 (ユーザ名だけの要点) および第 2 認証クライアントを成功フェーズに移動させます)。RADIUS 認証が (NAS として MAC アドレスおよび WLC 詳細と) 行われない場合、RADIUS コンフィギュレーションは確認されるべきです。

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...
Sep 10, 2017 08:37:37.891 AM	✓			ritmahaj	C0:EE:FB:D7:88:24	Unknown	Default >> D...	Default >> B...	PermitAccess
Sep 10, 2017 08:37:34.506 AM	✓			ritmahaj					